

Rec'd PCT/PTO 21 JAN 2005

#2

10/521789

PCT/JPO3/13405

日本国特許庁  
JAPAN PATENT OFFICE

21.10.03

RECEIVED  
04 DEC 2003  
WPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2002年10月25日

出願番号  
Application Number: 特願2002-311815  
[ST. 10/C]: [JP2002-311815]

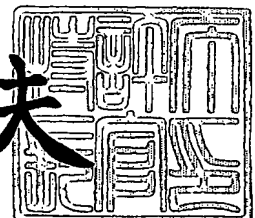
出願人  
Applicant(s): 松下電器産業株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2003年11月20日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 2931040030

【提出日】 平成14年10月25日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 伊藤 智祥

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山口 孝雄

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 佐藤 潤一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 武井 一朗

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100105050

【弁理士】

【氏名又は名称】 鷲田 公一

【手数料の表示】

【予納台帳番号】 041243

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9700376

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 透かし挿入装置および透かし取出装置

【特許請求の範囲】

【請求項 1】 プログラムの配布先ごとに異なる透かし情報を前記プログラムに挿入する透かし情報挿入手段と、前記透かし情報が改ざんされた場合には、前記プログラムを正しく動作させない透かし検証コードを前記プログラムに挿入するコード挿入手段と、を具備し、

前記透かし検証コードを前記配布先に関わらず同じにしたことを特徴とする透かし挿入装置。

【請求項 2】 前記透かし情報を、プログラムの配布先を一意に決定する ID 情報から生成することを特徴とする請求項 1 記載の透かし挿入装置。

【請求項 3】 前記透かし情報から所定の定数を出力する関数を定義し、前記関数を変数に代入する式を前記プログラムに挿入する関数挿入手段を具備し、

前記透かし検証コードは、前記変数と前記定数が等しいかどうかを判定し、等しくない場合にはプログラムを停止する条件分岐であり、

前記定数を前記配布先に関わらず同じにしていることを特徴とする請求項 1 または請求項 2 記載の透かし挿入装置。

【請求項 4】 前記透かし検証コードは、前記プログラムを正しく動作させるのに必要なものであることを特徴とする請求項 1 または請求項 2 記載の透かし挿入装置。

【請求項 5】 前記透かし検証コードは、前記プログラムから取り出した判定分岐に前記透かし情報から生成した前記判定分岐の判定文に影響を与えない計算式を挿入したものであることを特徴とする請求項 4 記載の透かし挿入装置。

【請求項 6】 請求項 1 から請求項 5 のいずれかに記載の透かし挿入装置が前記透かし情報および前記透かし検証コードを挿入したプログラムを入力するプログラム入力手段と、前記プログラムから前記透かし情報を取り出し、前記透かし情報に基づいて前記配布先を一意に特定する ID 情報を生成する透かし検出手段と、を具備し、

生成した前記 ID 情報に基づき配布先を特定することを特徴とする透かし取出

装置。

【請求項 7】 請求項 1 から請求項 5 のいずれかに記載の透かし挿入装置と、請求項 6 に記載の透かし取出装置と、を具備したことを特徴とするプログラム不正配布防止システム。

【請求項 8】 前記透かし挿入装置を前記配布先に設けたことを特徴とする請求項 7 記載のプログラム不正配布防止システム。

【請求項 9】 配布先ごとに異なる透かし情報を前記プログラムに挿入するステップと、前記透かし情報を用いたものであって、前記透かし情報が改ざんされた場合には、前記プログラムを正しく動作させないものであり、前記配布先に関わらず同じ透かし検証コードを前記プログラムに挿入するステップと、を具備したことを特徴とする透かし挿入方法。

【請求項 10】 プログラムの配布先ごとに異なる透かしをプログラムに挿入するステップと、前記透かし情報の挿入箇所の周辺もしくは前記プログラムの全体を仕様を変更することなく改変するステップと、を有することを特徴とする透かし挿入方法。

【請求項 11】 コンピュータに、プログラムの配布先ごとに異なる透かし情報を前記プログラムに挿入するステップと、前記透かし情報を用いたものであって、前記透かし情報が改ざんされた場合には、前記配布用プログラムを正しく動作させないものであり、前記配布先に関わらず同じ透かし検証コードを前記配布用プログラムに挿入するステップと、を行わせることを特徴とする透かし挿入プログラム。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、プログラムの不正な使用および配布を防止および抑止するためのプログラムへの透かしの挿入装置および透かし取出装置に関するものである。

##### 【0002】

#### 【従来の技術】

コンピュータネットワークの進展に伴い、ネットワークを介したコンピュータ

プログラムの流通が一般的になっている。コンピュータプログラムは、容易に複製を作成できるため、プログラムの複製が不正に2次配布されたり、プログラム中のアルゴリズムを盗用、改ざんされたりする可能性がある。したがって、このような不正利用からプログラムを保護する必要がある。

#### 【0003】

従来のプログラム保護の技術の一つとして、プログラムへ電子透かしを挿入する方法が挙げられる。この方法では、配布先ごとに異なる透かし情報をプログラムに埋め込んで配布することで、不正利用が発生した場合に流出元を容易に検出することが可能となる。

#### 【0004】

具体的な透かしの挿入方法としては、たとえば、特許文献1に開示されたものがある。

#### 【0005】

この方法は、まず、実行順序に依存関係のないコードを検出する。次に、検出部分にダミー変数の演算を挿入する。そして、ダミー変数の演算を含む検出部分の実行順序をランダムに入れ替える。

#### 【0006】

このような処理を行うことにより、その実行順序を電子透かし情報として配布先ごとに変更する仕組みを実現している。

#### 【0007】

##### 【特許文献1】

特開 2000-76064号公報

#### 【0008】

##### 【発明が解決しようとする課題】

しかしながら、従来のプログラムへの電子透かし挿入方式は、差分攻撃に基づく透かしの改変、削除が容易であるという問題がある。

#### 【0009】

差分攻撃とは、複数の電子透かしの挿入されたプログラムの差分をとることで、透かしデータの挿入箇所を特定する攻撃法である。

## 【0010】

従来の方式を用いて、プログラムに配布先ごとに異なる透かし情報を挿入した場合、各配布先に配布されたプログラムの中で差分をとると、透かしの挿入された個所だけが差分として浮かび上がってしまう。このように、差分攻撃で透かしの挿入位置が簡単に特定されてしまい、透かし情報の削除、改ざんが容易に可能であるという問題がある。

## 【0011】

本発明は、かかる点に鑑みてなされたものであり、透かしの挿入箇所を特定されないように透かしを挿入することにより、透かしがなく、かつ正常に動作するプログラムを容易に生成できないようにすることを目的とする。

## 【0012】

## 【課題を解決するための手段】

上記の課題を解決するための本発明は、プログラムの配布先を一意に特定するID情報から透かし情報を生成し、生成した透かし情報をプログラムに挿入し、透かし情報が改ざんされた場合にはプログラムを正しく動作させないものであり、かつ配布先に関わらず同じ透かし検証コードをプログラムに挿入するようにした。

## 【0013】

これにより、差分攻撃により透かしである透かし検証コードが検出されないようにできる。この結果、配布先は、透かしがなく、かつ正常に動作するプログラムを生成できないので、プログラムを不正に流通させることができなくなる。

## 【0014】

また、透かし情報を挿入したあとに、透かし挿入箇所周辺や、プログラム全体をプログラムの仕様が変更しない範囲で配布先ごとに異なるように改変するようにした。

## 【0015】

これにより、プログラムの差分を取った際に、透かし情報以外の部分が差分として浮かび上がるため、透かし挿入箇所を容易に特定することができなくなる。

## 【0016】

**【発明の実施の形態】**

本発明の第1の態様にかかる透かし挿入装置は、プログラムの配布先ごとに異なる透かし情報を前記プログラムに挿入する透かし情報挿入手段と、前記透かし情報が改ざんされた場合には、前記プログラムを正しく動作させない透かし検証コードを前記プログラムに挿入するコード挿入手段と、を具備し、前記透かし検証コードを前記配布先に関わらず同じにしたものである。

**【0017】**

このように透かし検証コードを配布先に関わらず同じにすることにより、差分攻撃により、透かし検証コードが差分として検出されないようにできる。これにより、差分攻撃により検出された箇所だけを改変、削除するという単純な手法では、透かし検証コードを改変、削除できなくなる。よって、配布先は、透かしがなく、かつ正常に動作するプログラムを生成できないので、プログラムを不正に流通させることができなくなる。

**【0018】**

本発明の第2の態様は、第1の態様にかかる透かし挿入装置において、配布先を一意に決定するID情報に基づき透かし情報を生成する。

**【0019】**

これにより、配布先が不正配布を行った際に、配布先を一意に特定することができ、プログラムの不正流通を防止できる。

**【0020】**

本発明の第3の態様は、第1の態様または第2の態様にかかる透かし挿入装置において、前記透かし情報から所定の定数を入力する関数を定義し、前記関数を変数に代入する式を前記プログラムに挿入する関数挿入手段を具備し、前記透かし検証コードは、前記変数と前記定数が等しいかどうかを判定し、等しくない場合にはプログラムを停止する条件分岐であり、前記定数を前記配布先に関わらず同じにしている。

**【0021】**

このような条件分布は、差分攻撃により検出されないので、差分攻撃により検出された箇所だけを改変、削除するという単純な手法では、全ての透かしを改変



、削除できなくなる。よって、配布先は、透かしがなく、かつ正常に動作するプログラムを生成できないので、プログラムを不正に流通させることができなくなる。

#### 【0022】

本発明の第4の態様は、第1の態様または第2の態様にかかる透かし挿入装置において、前記透かし検証コードは、前記プログラムを正しく動作させるのに必要なものである。

#### 【0023】

これにより、差分攻撃により検出した透かし情報から透かし検証コードを検出し、透かし検証コードを削除、改変してしまうとプログラムが正常に動作しないようになる。つまり、正常に動作する透かし情報のない（もしくは改変された）プログラムを生成することを不可能にすることができるので、プログラムの不正配布を防止できる。

#### 【0024】

本発明の第5の態様は、第4の態様にかかる透かし挿入装置において、前記透かし検証コードは、前記プログラムから取り出した判定分岐に前記透かし情報から生成した前記判定分岐の判定文に影響を与えない計算式を挿入したものである。

#### 【0025】

これにより、プログラムを正しく動作させるのに必要な透かし検証コードを入力できる。

#### 【0026】

本発明の第6の態様にかかる透かし取出装置は、第1の態様から第5の態様のいずれかに記載の透かし挿入装置が前記透かし情報および前記透かし検証コードを挿入したプログラムを入力するプログラム入力手段と、前記プログラムから前記透かし情報を取り出し、前記透かし情報に基づいて配布先を一意に特定するID情報を生成する透かし検出手段と、を具備し、生成した前記ID情報に基づき前記配布先を特定するものである。

#### 【0027】

これにより、不正にプログラムを流通した配布先を特定することができる。

#### 【0028】

本発明の第7の態様にかかるプログラム不正配布防止システムは、第1の態様から第5の態様のいずれかに記載の透かし挿入装置と、第6の態様に記載の透かし取出装置と、を具備した構成を採る。

#### 【0029】

このように第1の態様から第5の態様のいずれかに記載の透かし挿入装置と、第6の態様に記載の透かし取出装置と、を具備することにより、確実にプログラムの不正配布を防止できる。

#### 【0030】

本発明の第8の態様は、第7の態様にかかるプログラム不正配布防止システムにおいて、前記透かし挿入装置を前記配布先に設けたものである。

#### 【0031】

これにより、配布先に対して容易にプログラムを配布し、配布先において透かしを挿入するようにできる。このような形態は、単純にプログラムのみを配布することが好ましいシステムに効果的である。

#### 【0032】

本発明の第9の態様は、配布先ごとに異なる透かし情報を前記プログラムに挿入するステップと、前記透かし情報を用いたものであって、前記透かし情報が改ざんされた場合には、前記プログラムを正しく動作させないものであり、前記配布先に関わらず同じ透かし検証コードを前記プログラムに挿入するステップと、を具備したことを特徴とする透かし挿入方法である。

#### 【0033】

本発明の第10の態様は、プログラムの配布先ごとに異なる透かしをプログラムに挿入するステップと、前記透かし情報の挿入箇所の周辺もしくは前記プログラムの全体を仕様を変更することなく改変するステップと、を有することを特徴とする透かし挿入方法である。

#### 【0034】

これにより、プログラムの差分をとったときに、透かし以外の部分が差分とし

て検出されるため、差分攻撃に基づいて透かし挿入位置を特定することが困難になる。この結果、透かし改変、削除を確実に防ぐことができ、プログラムの不正流通を防止できる。

#### 【0035】

本発明の第11の態様は、コンピュータに、プログラムの配布先ごとに異なる透かし情報を前記プログラムに挿入するステップと、前記透かし情報を用いたものであって、前記透かし情報が改ざんされた場合には、前記配布用プログラムを正しく動作させないものであり、前記配布先に関わらず同じ透かし検証コードを前記配布用プログラムに挿入するステップと、を行わせることを特徴とする透かし挿入プログラムである。

#### 【0036】

##### (実施の形態1)

本発明の実施の形態1にかかる透かし挿入装置および透かし取出装置を具備したプログラム不正配布防止システムについて添付図面を用いて説明する。

#### 【0037】

図1は、実施の形態1にかかる透かし挿入による不正配布防止システムの構成図である。

#### 【0038】

まず、配布先10は、プログラム配布の際に、透かし挿入装置20により、配布先40a、40bごとに、異なる透かしを挿入して配布する（配布先の2次配布を認めないものとする）。

#### 【0039】

このように透かしを埋め込んで配布することで、不正な2次配布などプログラムが流出した際に、配布元10は、透かし取出装置30を用いて、流出先50に流出したプログラムから透かしを取り出して配布先を確認し、流出元（配布先）40a、40bを特定することができる。

#### 【0040】

また、配布先40a、40bは、透かしによる流出元の特定を恐れて、不正な2次配布を控えることになる。

**【 0 0 4 1 】**

このようにして、不正配布防止システムは、透かしによる不正配布を抑止する。

**【 0 0 4 2 】**

次に、実施の形態 1 にかかる透かし挿入装置 2 0 について図 2 を用いて説明する。図 2 は、実施の形態 1 の透かし挿入装置の構成図である。

**【 0 0 4 3 】**

透かし挿入装置 2 0 には、プログラム入力部 2 0 1 が設けられている。プログラム入力部 2 0 1 は、透かしを入力するプログラムコードを入力する手段である。プログラム入力部 2 0 1 は、プログラムコードを透かし挿入部 2 0 2 に出力する。

**【 0 0 4 4 】**

透かし挿入部 2 0 2 は、ID 情報生成部 2 0 5 により生成される ID 情報からプログラムに実際に埋め込む透かしを生成し、プログラム入力部 2 0 1 から出力されたプログラムコードに対し、透かしを入力する手段である。また、透かし挿入部 2 0 2 は、プログラム入力部 2 0 1 が出力したプログラムコードがソースコードであれば、ソースコードをコンパイルし、透かしの入力箇所をアセンブラコードの行番号として透かし情報記録部 2 0 6 に渡す。

**【 0 0 4 5 】**

プログラム出力部 2 0 3 は、透かし挿入部 2 0 2 が透かしを入力したプログラムコードを出力する手段である。

**【 0 0 4 6 】**

透かし用データ入力部 2 0 4 は、透かし用データを入力する。入力する透かし用データは、配布先を一意に特定する情報であり、配布先の住所、電話番号、会社名、氏名、電子メールアドレスなどである。また、透かし用データに、配布元の情報を入力してもよい。

**【 0 0 4 7 】**

ID 情報生成部 2 0 5 は、透かし用データ入力部 2 0 4 により入力された透かし用データから一意に決定できる ID 情報を生成する。ID 情報は、入力したデ

ータそのものであってもよいし、それを暗号化したデータであってもよい。また、ID情報は、透かし用データを保存するデータベース上において透かし用データを一意に特定するためのIDであってもよい。

#### 【0048】

なお、本発明の実施の形態においては、ID情報に基づいて透かし情報を生成する形態となっているが、必ずしもID情報に基づいて透かし情報を生成する必要はなく、透かし情報から一意に配布先を特定可能となっていれば良い。例えば、ソフトウェアに1～Nシーケンス番号を透かし情報として挿入し、配布先Aにシーケンス番号iのソフトを配布、配布先Bにシーケンス番号jのソフトを配布といったように透かし情報と配布先を一意に特定可能としてもよい。

#### 【0049】

透かし情報記録部206は、透かし挿入部202が挿入した透かしの挿入箇所を記録する手段である。具体的には、透かしを挿入したコードのアセンブラコード行番号を記録する。

#### 【0050】

次に、実施の形態1にかかる透かし取出装置30について図3を用いて説明する。図3は、実施の形態1における、透かし取出装置30の構成図である。

#### 【0051】

プログラム入力部301は、透かしを挿入したプログラムを入力する手段である。

#### 【0052】

透かし検出部302は、プログラム入力部301から出力されたプログラムを逆アセンブリングし、透かし情報記憶部305より得られる透かし挿入箇所（アセンブラコード行番号）から入力された透かしを取り出す。そして、透かし検出部302は、取り出した透かしからID情報を生成し、ID情報記憶部305に渡す。

#### 【0053】

ID情報記憶部304は、透かし検出部302より得られるID情報から、配布先の情報を生成する手段である。ID情報記憶部304は、ID情報がデータ

ベースのデータのIDである場合には、IDからデータを取り出すことで、配布先の情報を取得する。また、ID情報記憶部304は、ID情報が配布先の情報の暗号化データである場合には、復号して配布先の情報を取得する。

#### 【0054】

透かし情報記憶部305は、配布したプログラムの透かし挿入箇所を記憶している手段である。透かし挿入箇所の情報は、透かし挿入装置20の透かし情報記録部206より得る。

#### 【0055】

出力部303は、取得された配布先の情報を出力する手段である。

#### 【0056】

次に、実施の形態1にかかる透かし挿入部202の透かし挿入動作について図4を用いて説明する。図4は、実施の形態1にかかる透かし挿入部202の動作を表すフローチャートである。

#### 【0057】

まず、透かし挿入部202は、配布先40の情報から生成されるID情報Iから、実際にプログラムに挿入する透かし情報X1、X2を生成関数F1により生成する(ステップ401)。

#### 【0058】

続いて、透かし挿入部202は、透かし情報X1、X2を入力としたとき、定数C1を出力する関数F21および定数C2を出力する関数F22を構成する(ステップ402)。

#### 【0059】

続いて、透かし挿入部202は、透かし情報X1、X2を変数val1, val12に代入する式をプログラムコード中に埋め込む(ステップ403)。

#### 【0060】

続いて、透かし挿入部202は、プログラムコード中に、F21(val1, val2)を変数val3に、F22(val1, val2)を変数val4に代入する式を埋め込む(ステップ404)。

#### 【0061】

続いて、透かし挿入部 202 は、透かし検証コードである、変数  $v a 1 3$  と定数  $C 1$  が等しいかどうかを判定し、等しくない場合にはプログラムを停止する条件分岐と、変数  $v a 1 4$  と定数  $C 2$  が等しいかどうかを判定し、等しくない場合にはプログラムを停止する条件分岐と、をプログラムコード中に埋め込む（ステップ 405）。

#### 【0062】

そして、透かし挿入部 202 は、ステップ 403 からステップ 405 において透かし情報および透かし検証コードを挿入した箇所を透かし情報記録部 206 に記録する（ステップ 406）。

#### 【0063】

このようにして、透かし挿入部 202 は、プログラムに透かしである透かし情報および透かし検証コードを挿入する。

#### 【0064】

なお、透かし挿入部 202 は、ステップ 403 からステップ 405 において、挿入した式および条件分岐（透かし検証コード）を、プログラムの実行順に入力する。ただし、 $F 1$  は、 $X 1$ 、 $X 2$  より  $I$  を一意に生成する  $F 1$  の逆関数を持つことを条件とし、 $F 2 1$ 、 $F 2 2$  は、 $F 2 1(X 1, X 2) == C 1$  かつ  $F 2 2(X 1, X 2) == C 2$  を  $X 1$ 、 $X 2$  以外の時には満たさないことを条件とする（“==” は値が等しいことをあらわす。）。

#### 【0065】

たとえば、 $I D$  情報  $I = 1 2 3 4 5 6 7 8$ 、 $F 1$  は 8 桁の値を 4 桁目から 2 つの値に分割する関数、 $F 2 1(x, y)$ 、 $F 2 2(x, y)$  は  $a x + b y$  という 2 変数一次関数、 $C 1 = 2 3 4 5$ 、 $C 2 = 5 6 7 8$  の場合を考える。

#### 【0066】

この場合、まず、 $F 1$  から、透かし情報  $X 1 = 1 2 3 4$ 、 $X 2 = 5 6 7 8$  が生成される。また、 $F 2 1$ 、 $F 2 2$  は、 $a 1 \times 1 2 3 4 + b 1 \times 5 6 7 8 = 2 3 4 5$ 、 $a 2 \times 1 2 3 4 + b 2 \times 5 6 7 8 = 5 6 7 8$  を満たす  $a 1$ 、 $a 2$ 、 $b 1$ 、 $b 2$  を求めることにより構成する。たとえば、 $a 1 = 1$ 、 $a 2 = 0.195667$ 、 $b 1 = 3.700972$ 、 $b 2 = 0.195667$  は条件を満たす。

## 【0067】

次に、実施の形態1を適用した場合に生成されるプログラムの例を、図5に示す。

## 【0068】

500aは、プログラム入力部201が入力した基本となる基本プログラムである。プログラム500b、500cは、基本プログラム500aに透かしである透かし情報および透かし検証コードを入力した透かし挿入プログラムである。

## 【0069】

まず、透かし挿入部202は、ステップ403において、透かし挿入プログラム500b、500cに、それぞれ別のID情報Ia(12345678)、Ib(11112222)より生成された透かし情報X1a(1234)、X1b(5678)とX2a(1111)、X2b(2222)を入力する(図中501に示す部分)。

## 【0070】

次に、透かし挿入部202は、ステップ404において、透かし挿入プログラム500b、500cに、それぞれ別のF21、F22を透かし挿入プログラム500b、500cに挿入する(図中502に示す部分)。

## 【0071】

そして、透かし挿入部202は、ステップ405において、透かし検証コードとして、変数val3と定数C1(2345)が等しいかどうかを判定し、等しくない場合にはプログラムを停止する条件分岐(assert(0))と、変数val4と定数C2(5678)が等しいかどうかを判定し、等しくない場合にはプログラムを停止する条件分岐(assert(0))と、をプログラムコード中に埋め込む(図中503に示す部分)。

## 【0072】

ここで、着目すべき点は、2つのプログラム500bと500cの差分をとると、透かし情報である501、502の部分は検出されるが、透かし検証コードである条件分岐503は検出されないことである。これにより、プログラム500b、500cに差分攻撃をすることにより、透かし入力箇所を検出し、検出部



分の改ざん、削除を行ったとしても、透かし検証コードである条件分岐 5 0 3 の部分の改ざん、削除は行えない。よって、透かし検証コード 5 0 3 の部分が条件と合わなくなり、プログラムが動作しなくなる。

#### 【0 0 7 3】

このように、差分攻撃により検出された箇所だけを改変、削除するという単純な手法では、全ての透かしを削除した正常に動作するプログラムを入手できなくさせることが可能となる。

#### 【0 0 7 4】

なお、わかりやすさのため、図 5 ではソースコードを用いて説明しているが、バイナリコードの場合でも同じことが言える。また、図 5 では、条件分岐 5 0 3 は、条件文が真であった場合にプログラムを停止するように処理しているが、そうでなく、プログラムが異常な動作をするように（たとえば、a ++ とするなど）プログラム中の変数値を変更するように処理することもできる。

#### 【0 0 7 5】

さらに、実施の形態 1 では、ID 情報から、2 つの透かし情報を生成しているが、3 つ以上の透かし情報を生成することとしてもよい。

#### 【0 0 7 6】

次に、実施の形態 1 にかかる透かし検出部 3 0 2 の動作について図 6 を用いて説明する。図 6 は、実施の形態 1 の透かし検出部 3 0 2 の動作を表すフローチャートである。

#### 【0 0 7 7】

まず、透かし検出部 3 0 2 は、プログラムの実行コードを逆アセンブルする（ステップ 1 0 0 1）。

#### 【0 0 7 8】

その後、透かし検出部 3 0 2 は、透かし情報記憶部 3 0 5 を参照し、プログラムへの透かし挿入箇所を記録した記録情報（挿入箇所を示すアセンブラ行番号）を取得し、これに基づいて透かし情報 X 1、X 2 の入力箇所を特定する。そして、透かし検出部 3 0 2 は、透かし情報 X 1、X 2 をプログラムから取り出す（ステップ 1 0 0 2）。

## 【0079】

続いて、透かし検出部302は、透かし情報X1、X2を生成する際に使用した関数F1の逆関数を使用して、ID情報Iを生成する（ステップ1003）。

## 【0080】

このようにして、透かし検出部302は、ID情報Iを取得して、配布先40の特定を行う。

## 【0081】

なお、上記の方法では、実行コードの配布先もしくは流出先で、最適化、難読化といった処理によりコードの実行順番を入れ替えられた場合に、透かし情報の入力箇所のアセンブラ行番号が変化してしまい、透かし情報を得られない可能性がある。このような場合を考慮して、ステップ1002の処理を、挿入箇所を示すアセンブラ行番号の周辺の行において、代入命令をさがし、代入命令のオペランド部を取り出すという処理に変更してもよい。

## 【0082】

以上説明したように、実施の形態1によれば、透かし検証コード（図5の503の部分）は、配布先に関わらず同じなので、差分攻撃により、透かし検証コード（図5の503の部分）が差分として検出されないようにできる。これにより、差分攻撃により透かし検証コードの挿入位置を検出することができない。この結果、差分攻撃により検出された箇所だけを改変、削除するという単純な手法では、全ての透かしを改変、削除できなくなり、正常に動作する透かしのない（もしくは改変された）プログラムを生成することが不可能になる。よって、配布先は、透かしがなく、かつ正常に動作するプログラムを生成できないので、プログラムを不正に流通させることができなくなる。

## 【0083】

なお、透かし挿入装置20および透かし取出装置30の行う処理をプログラムにし、汎用のコンピュータに実行させる形態であってもよい。

## 【0084】

（実施の形態2）

本発明の実施の形態2は、不正にプログラムを配信しようとした者が、差分攻

撃により透かし情報を検出し、検出した透かし情報に用いられている関数により生成される変数を使用している箇所（図5に示す503の部分）を検出し、検出した箇所を改変、削除することにより、実施の形態1の透かし検証コードを改変、削除しようとした場合に対応したものである。

#### 【0085】

具体的には、透かし情報を用いたものであり、かつプログラムを正しく動作させるのに必要な透かし検証コードをプログラム中に挿入するようにしたものである。

#### 【0086】

これにより、上述した手順により透かし情報を用いた透かし検証コードを検出し、改変、削除した場合には、プログラムを正常に動作させなくすることができる。

#### 【0087】

以下、実施の形態2について詳細に説明する。実施の形態2における透かし挿入装置と、実施の形態1における透かし挿入装置20との違いは、透かし挿入部202の動作である。

#### 【0088】

次に、実施の形態2の透かし挿入部の動作について図7を用いて説明する。図7は、実施の形態2の透かし挿入部の動作のフローチャートである。

#### 【0089】

ステップ601およびステップ602の動作は、実施の形態1で説明した図4のステップ401およびステップ402の動作と同様であるので説明を省略する。

#### 【0090】

続いて、透かし挿入部は、透かし情報X1、X2より、 $C1 + C2 + C3 = 0$ となるC3を生成する関数F3を生成する（ステップ603）。

#### 【0091】

続いて、透かし挿入部は、透かし情報X1、X2を変数val1, val2に代入する式をプログラムコード中に埋め込む（ステップ604）。

## 【0092】

続いて、透かし挿入部は、プログラムコード中に、F21 (val1, val2) を変数 val3 に、F22 (val1, val2) を変数 val4 に代入する式を埋め込む (ステップ605)。

## 【0093】

続いて、透かし挿入部は、透かし検証コードとして、変数 val3 と定数 C1 が等しいかどうかを判定し、等しくない場合にはプログラムを停止する条件分岐と、変数 val4 と定数 C2 が等しいかどうかを判定し、等しくない場合にはプログラムを停止する条件分岐と、をプログラムコード中に埋め込む (ステップ606)。

## 【0094】

続いて、透かし挿入部は、F3 (val1, val2) を変数 val5 に代入する式を埋め込む (ステップ607)。

## 【0095】

次に、透かし挿入部は、透かし検証コードとして、 $val3 + val4 + val5$  をオリジナルコードの 0 を判定する判定文に加算するコードをプログラム中に挿入する (ステップ608)。

## 【0096】

そして、透かし挿入部202は、ステップ604からステップ608において透かし情報および透かし検証コードを挿入した箇所を透かし情報記録部206に記録する (ステップ609)。

## 【0097】

このようにして、透かし挿入部は、プログラムに透かしを挿入する。

## 【0098】

ここで、着目すべき点は、ステップ608で挿入される  $val3 + val4 + val5$  には、差分検出で検出される変数、val3、val4、val5が含まれている点であり、 $val3 + val4 + val5$  がプログラムの動作に関わる判定文の 0 の部分に挿入されている点である。これにより、不正使用者が、差分攻撃により変数 (val3、val4、val5) を検出し、検出した変数を

用いている関数により生成される変数を使用している箇所を改変、削除しようとした場合に、プログラムの動作にかかわる判定文も改変、削除してしまうことになる。よって、プログラムが正常に動作しなくなり、不正使用もできなくなる。

#### 【0099】

次に、実施の形態2にかかる透かし挿入部が生成したプログラムについて図8を用いて説明する。

#### 【0100】

800aは、プログラム入力部201が入力した基本となる基本プログラムである。プログラム800bは、基本プログラム800aに透かしを入力した透かし挿入プログラムである。

#### 【0101】

プログラム800bには、ステップ604において、701で示される部分に透かし情報が挿入され、ステップ605、ステップ607において、702で示される部分に透かし検証用の計算式（コード）が挿入される。

#### 【0102】

そして、プログラム800bには、703で示される部分に、ステップ608の処理結果が挿入される。また、プログラム800bには、ステップ606において、704で示される部分に透かし検証コードが挿入される。

#### 【0103】

このようにプログラム800bを生成することにより、不正に使用しようとした者が、差分攻撃によりプログラム800bから透かし検証コード703を検出し、透かし検証コードを改変、削除すると、透かし検証コード703は、仕様（オリジナルの祖コードにおける、プログラムの入出力関係）に関連するコードであるので、このコードを削除するとプログラムが正しく動作しなくなる。

#### 【0104】

透かしのうち、透かし検証コード703の判定文のみ変更しようとするためにはプログラムの仕様を理解して、透かし検証コード703が仕様に関連あるコードであることを知る必要がある。これは、プログラムの構造を理解した物が、時間をかけて行う必要があり、機械的な処理により透かしの削除はできない。

## 【0105】

なお、 $C1 + C2 + F3 = 0$ でなくても良い。ただし、この場合は、 $C1 + C2 + F3$ により得られる値を用いた判定文に $C1 + C2 + F3$ を挿入すればよい。例えば、 $C1 + C2 + F3 = 1$ である場合は、1を判定する判定文の1を $C1 + C2 + F3$ を置換する。

## 【0106】

以上説明したように、実施の形態2によれば、差分攻撃により検出した透かし情報（701、702）に用いられている関数により生成される変数を使用している箇所（図8に示す703の部分）を検出し、改変、削除した場合に、プログラムが正常に動作しないようになる。つまり、正常に動作する透かしのない（もしくは改変された）プログラムを生成することを不可能にすることができるので、プログラムの不正配布を防止できる。

## 【0107】

（実施の形態3）

本発明の実施の形態3は、透かし情報および透かし検証コードを入力した箇所周辺のコード、もしくはコード全体を難読化などの処理をすることにより改変するものである。これにより、差分攻撃により透かし以外のコードが検出されてしまうので、差分攻撃に基づく透かし改変、削除を確実に防ぐことができる。

## 【0108】

以下、実施の形態3について詳細に説明する。実施の形態3における透かし挿入装置と、実施の形態1における透かし挿入装置20との違いは、透かし挿入部202の動作である。

## 【0109】

次に、実施の形態3の透かし挿入部の動作について図9を用いて説明する。図9は、実施の形態3の透かし挿入部の動作フローチャートである。

## 【0110】

まず、透かし挿入部は、変数*i*に初期値1を代入する（ステップ800）。次に、透かし挿入部は、ID情報を*n*個の情報に分割して、透かし情報X（1），X（2）…X（*n*）を生成する（ステップ801）。

## 【0111】

続いて、透かし挿入部は、プログラムソースコード中のループ部（`while`、`for`文）を検出し（ステップ802）、ループの内部に透かし情報X（i）を挿入する（ステップ803）。

## 【0112】

その後、透かし挿入部は、“ループを含むプログラムを難読化する方法の提案”，（門田ら，信学論D-I， Vol. J80-D-I， No. 7， pp. 644-652， July 1997）に記載される方法を適用することで、挿入箇所のループ部を難読化する（ステップ804）。この際、プログラムの難読化の仕方に複数のバリエーションがあるが、バリエーションをランダム（もしくは過去に配布したプログラムに施した難読化と重ならないよう）に選択する。

## 【0113】

そして、透かし挿入部は、変数iが透かし情報の数n以下か判断し（ステップ805）、変数iがn以下の場合は変数iをインクリメントし（ステップ806）、ステップ802の処理に以降する。一方、ステップ805において、変数iがn以下でないと判断した場合、つまり全ての透かし情報を入力した場合は、透かし挿入部は、その後ソースコードをコンパイルし、透かし情報が入力されたアセンブラコードの行番号を記録してプログラムを出力し、処理を終了する（ステップ807）。

## 【0114】

次に、実施の形態3にかかる透かし挿入部が生成したプログラムについて図10を用いて説明する。900aは、プログラム入力部201が入力した基本となる基本プログラムである。プログラム900b、900cは、基本プログラム900aに透かし情報901を入力した透かし挿入プログラムである。

## 【0115】

プログラム900b、900cには、難読化により、実装は異なるものの、仕様（プログラムの入出力の関係）は変化していない。プログラム900b、900cの差分をとると、透かし以外の場所もプログラムコードが変化しているため

、透かし以外の部分 902 a、902 b も差分として検出される。

#### 【0116】

したがって、プログラム 900 b、900 c の透かしを改変、削除するためには、プログラムを解析し、どの部分がプログラムの仕様に関係のない透かしとなっているかを探し出す必要がある。プログラムの仕様に関係ない部分であるかどうかを判定するためには、プログラムの仕様を理解する必要があるため、この方法により埋め込まれた透かしを機械的に削除することは困難となる。

#### 【0117】

以上説明したように、実施の形態 3 によれば、差分攻撃により透かし以外のコードであるプログラムの仕様に関係する部分が検出されるため、差分攻撃に基づいて透かし挿入位置を特定することが困難になる。この結果、透かし改変、削除を確実に防ぐことができ、プログラムの不正流通を防止できる。

#### 【0118】

(実施の形態 4)

本発明の実施の形態 4 は、配布先に透かし挿入装置を保持し、配布したプログラムに対して配布先で透かしを付与するものである。

#### 【0119】

以下、実施の形態 4 にかかる不正配布防止システムの構成について図 11 を用いて説明する。図 11 は、実施の形態 4 にかかる透かし挿入による不正配布防止システムの構成図である。なお、すでに説明した部分と同一の部分には同一の符号を付与してある。

#### 【0120】

本システムでは、まず、配布元 1100 が、配布先 1110、1120 に対して、それぞれ配布先 1110、1120 を一意に決定する ID 情報 1101、1102 を配布する。

#### 【0121】

これに対して、配布先 1110、1120 の透かし挿入装置 20 a、20 b では、ID 情報 1101、1102 を記録しておく。

#### 【0122】



続いて、配布元 1 1 0 0 は、配布先 1 1 1 0、1 1 2 0 にプログラム 1 1 0 3 を配布する。

#### 【0 1 2 3】

これに対して、配布先 1 1 1 0、1 1 2 0 では、配布されたプログラム 1 1 0 3 に対して、透かし挿入装置 2 0 a、2 0 b を利用して透かしを挿入したプログラム 1 1 1 1、1 1 2 1 を生成する。

#### 【0 1 2 4】

なお、透かし挿入装置 2 0 a、2 0 b は、実施の形態 1 から実施の形態 3 のいずれかにかかるものであってもよい。

#### 【0 1 2 5】

その後、透かし挿入装置 2 0 a、2 0 b は、透かしを挿入した箇所を記録した記録情報 1 1 0 4、1 1 0 5 を配布元 1 1 1 0、1 1 2 0 に送信し、配布元 1 1 0 0 では記録情報 1 1 0 4、1 1 0 5 を保存する。

#### 【0 1 2 6】

配布元 1 1 0 0 は、配布先 1 1 1 0 が、流出先 1 1 3 0 に不正な 2 次配布を行った場合には、流出したプログラム 1 1 1 2 を取得し、記録情報 1 1 0 4、1 1 0 5 とともに透かし取出装置 3 0 に入力する。そして、配布元 1 1 0 0 は、透かし取出装置 3 0 において、配布先 1 1 1 0、1 1 2 0 を特定する ID 情報 1 1 0 7 を入手する。そして、配布元 1 1 0 0 は、配布先 1 1 1 0、1 1 2 0 に配布した ID 情報 1 1 0 1、1 1 0 2 と、入手した ID 情報 1 1 0 7 を比較し、不正にプログラムを流出した配布先 1 1 1 0、1 1 2 0 を特定する。

#### 【0 1 2 7】

以上説明したように、実施の形態 4 によれば、不特定多数の配布先に対して容易にプログラムを配布し、配布先において透かしを挿入するようにできる。このような形態は、単純にプログラムのみを配布することが好ましいシステム、たとえばデジタル放送を利用したプログラムの配布であるとか、IP ネットワークでマルチキャスト、ブロードキャストを利用したプログラム配布などに適用すると効果的である。

#### 【0 1 2 8】

**【発明の効果】**

以上説明したように、本発明によれば、透かしの挿入箇所を特定することが困難なように透かしを挿入できるので、透かしがなく、かつ正常に動作するプログラムを生成できないようにできる。

**【図面の簡単な説明】****【図 1】**

本発明の実施の形態 1 にかかる透かし挿入による不正配布防止システムの構成図

**【図 2】**

実施の形態 1 の透かし挿入装置の構成図

**【図 3】**

実施の形態 1 における、透かし取出装置の構成図

**【図 4】**

実施の形態 1 にかかる透かし挿入部の動作を表すフローチャート

**【図 5】**

実施の形態 1 を適用した場合に生成されるプログラムを示す図

**【図 6】**

実施の形態 1 の透かし検出部の動作を表すフローチャート

**【図 7】**

本発明の実施の形態 2 にかかる透かし挿入部の動作のフローチャート

**【図 8】**

実施の形態 2 にかかる透かし挿入部が生成したプログラムを示す図

**【図 9】**

本発明の実施の形態 3 にかかる透かし挿入部の動作フローチャート

**【図 10】**

実施の形態 3 にかかる透かし挿入部が生成したプログラムを示す図

**【図 11】**

本発明の実施の形態 4 にかかる透かし挿入による不正配布防止システムの構成図

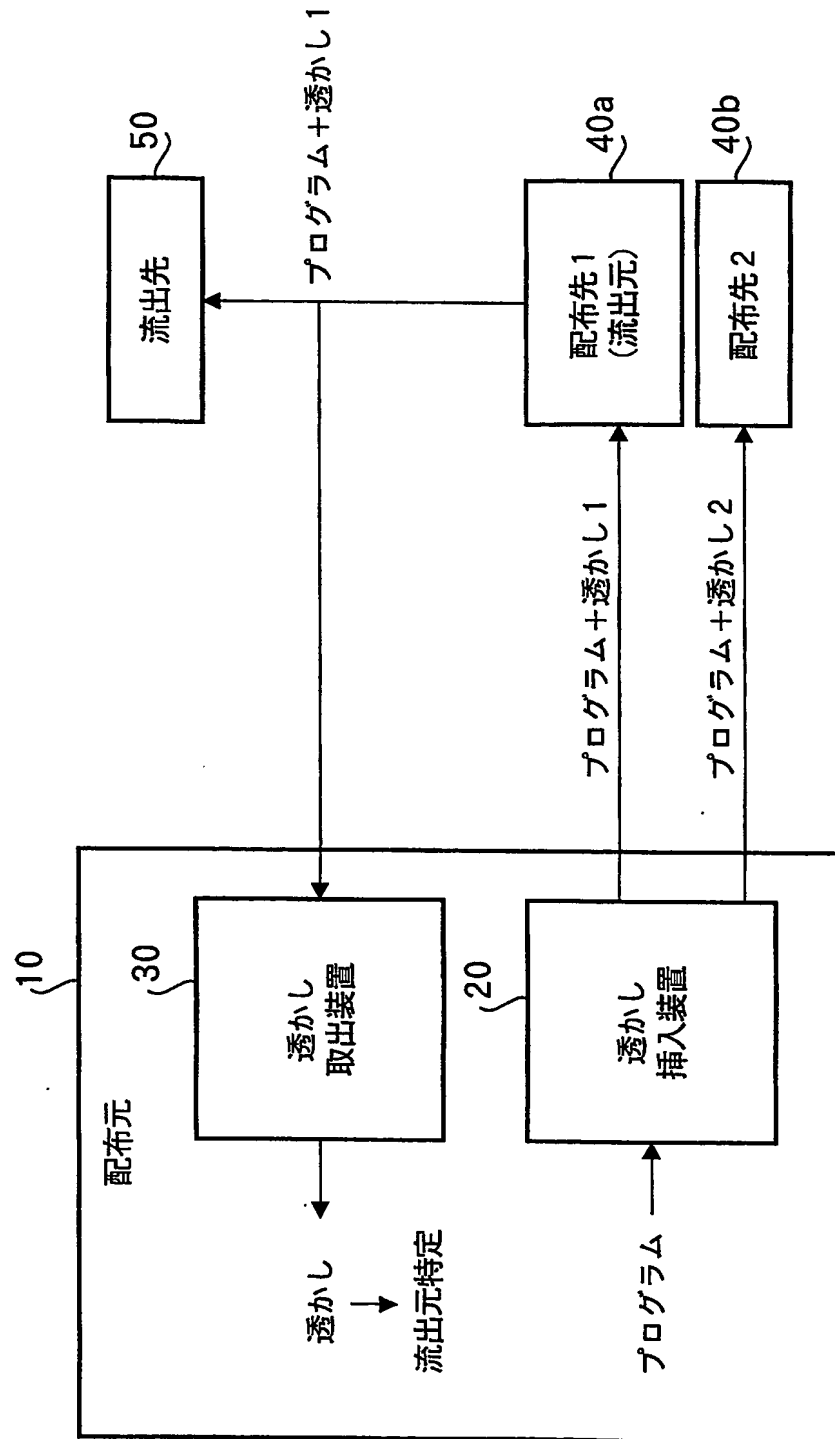
## 【符号の説明】

1 0、1 1 1 0 0 配布元  
2 0 透かし挿入装置  
3 0 透かし取出装置  
4 0 a、4 0 b、1 1 1 0、1 1 2 0 配布先  
5 0、1 1 3 0 流出先  
2 0 1、3 0 1 プログラム入力部  
2 0 2 透かし挿入部  
2 0 3 プログラム出力部  
2 0 4 透かし用データ入力部  
2 0 5 I D 情報生成部  
2 0 6、3 0 5 透かし情報記憶部  
3 0 2 透かし検出部  
3 0 3 出力部  
3 0 4 I D 情報記憶部

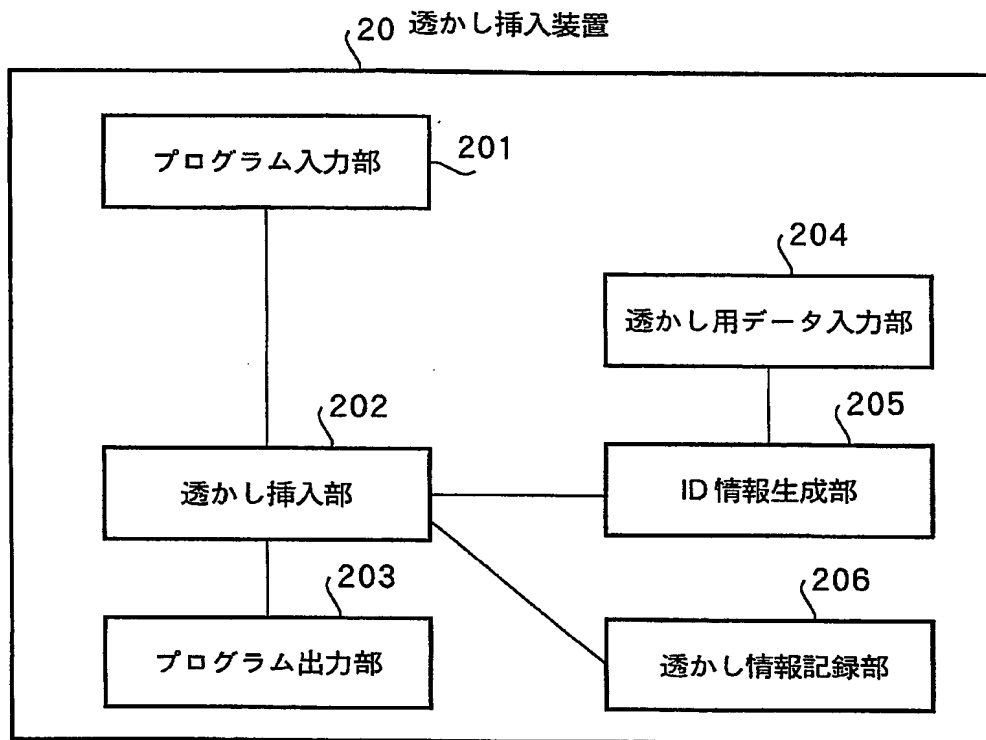
【書類名】

図面

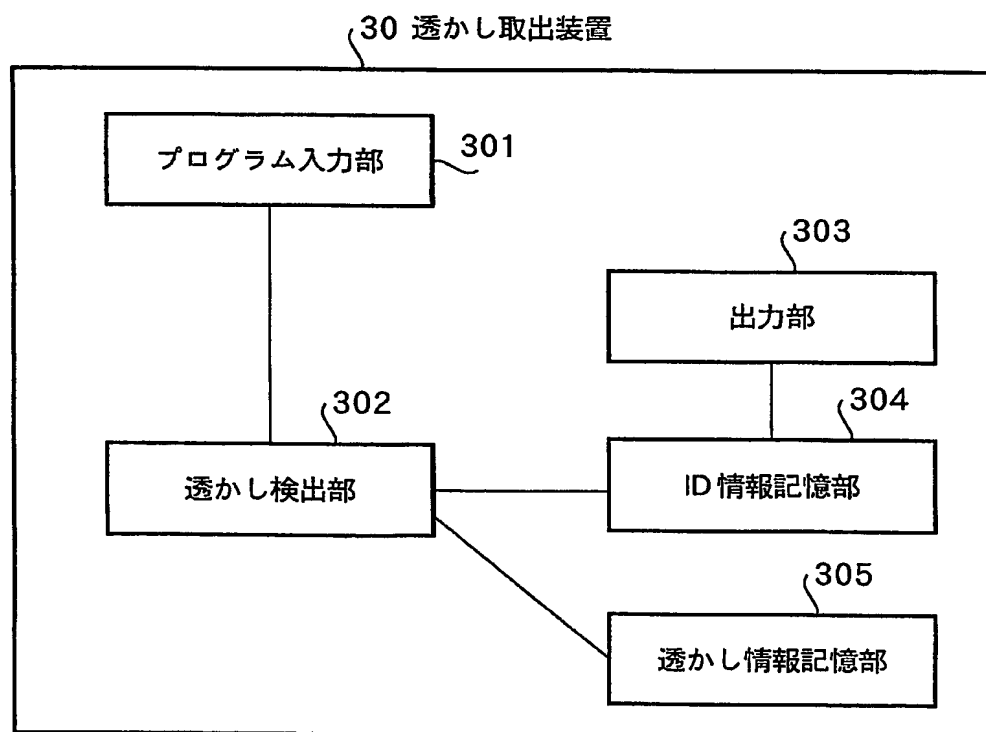
【図 1】



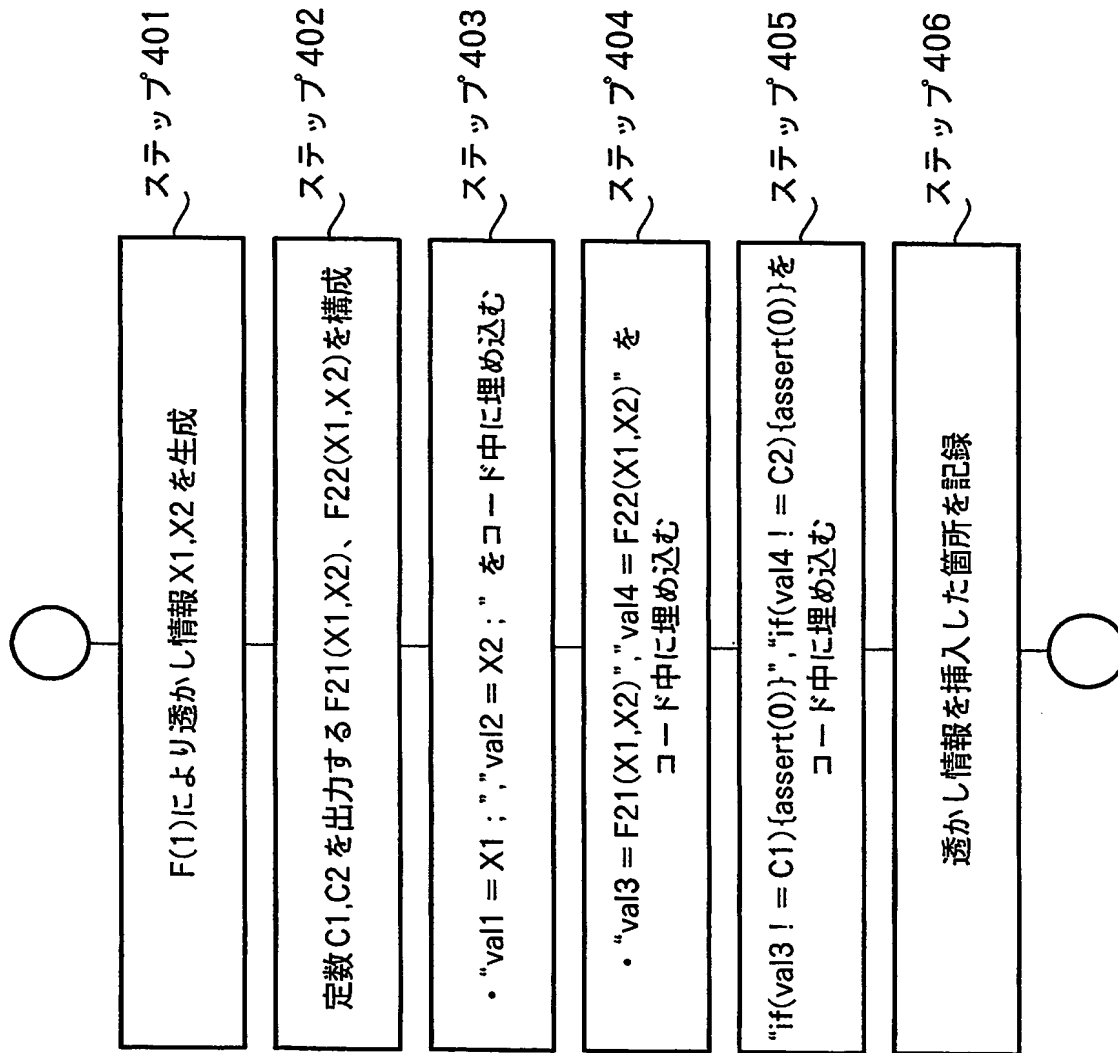
【図 2】



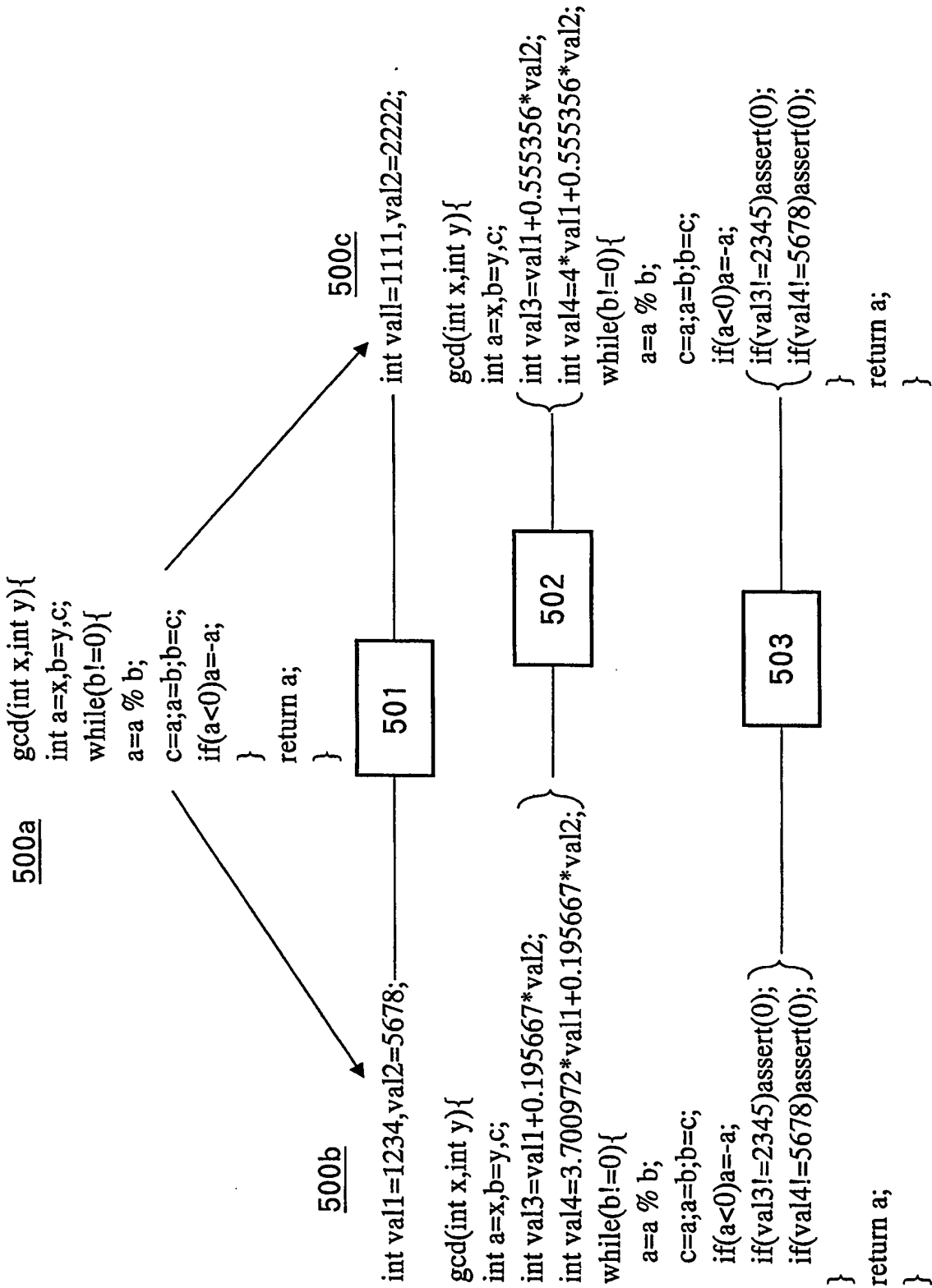
【図 3】



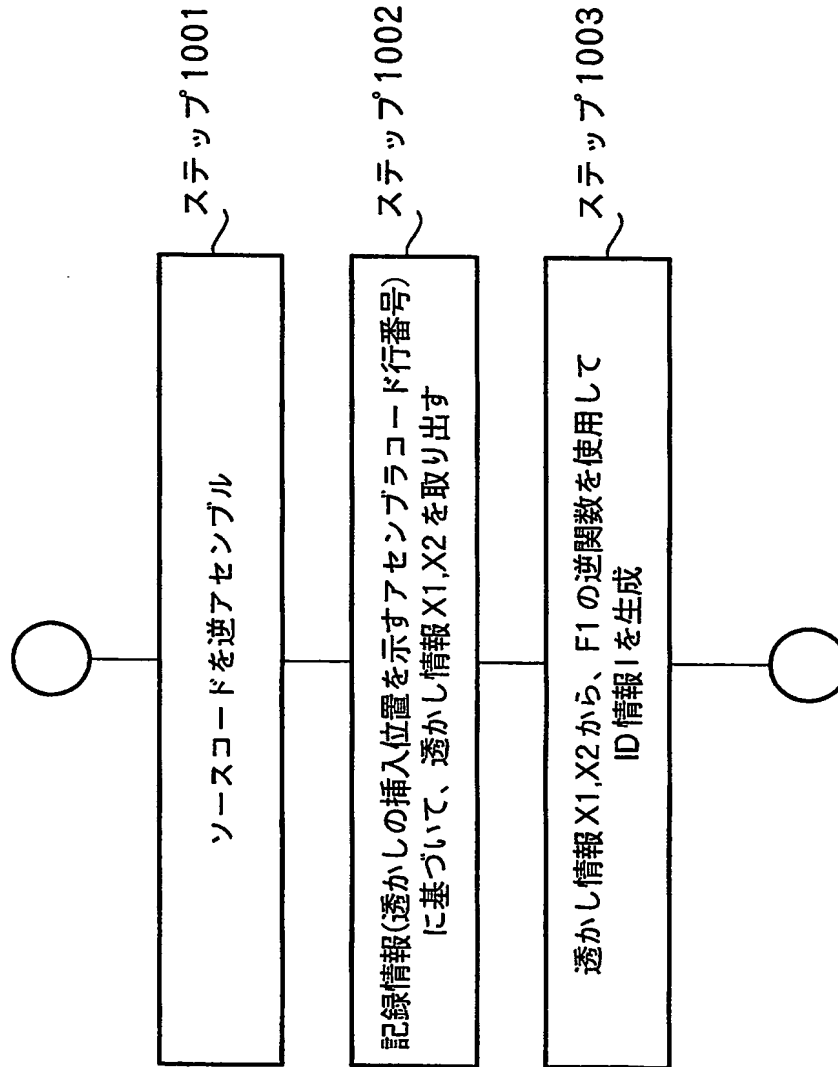
【図 4】



【図 5】

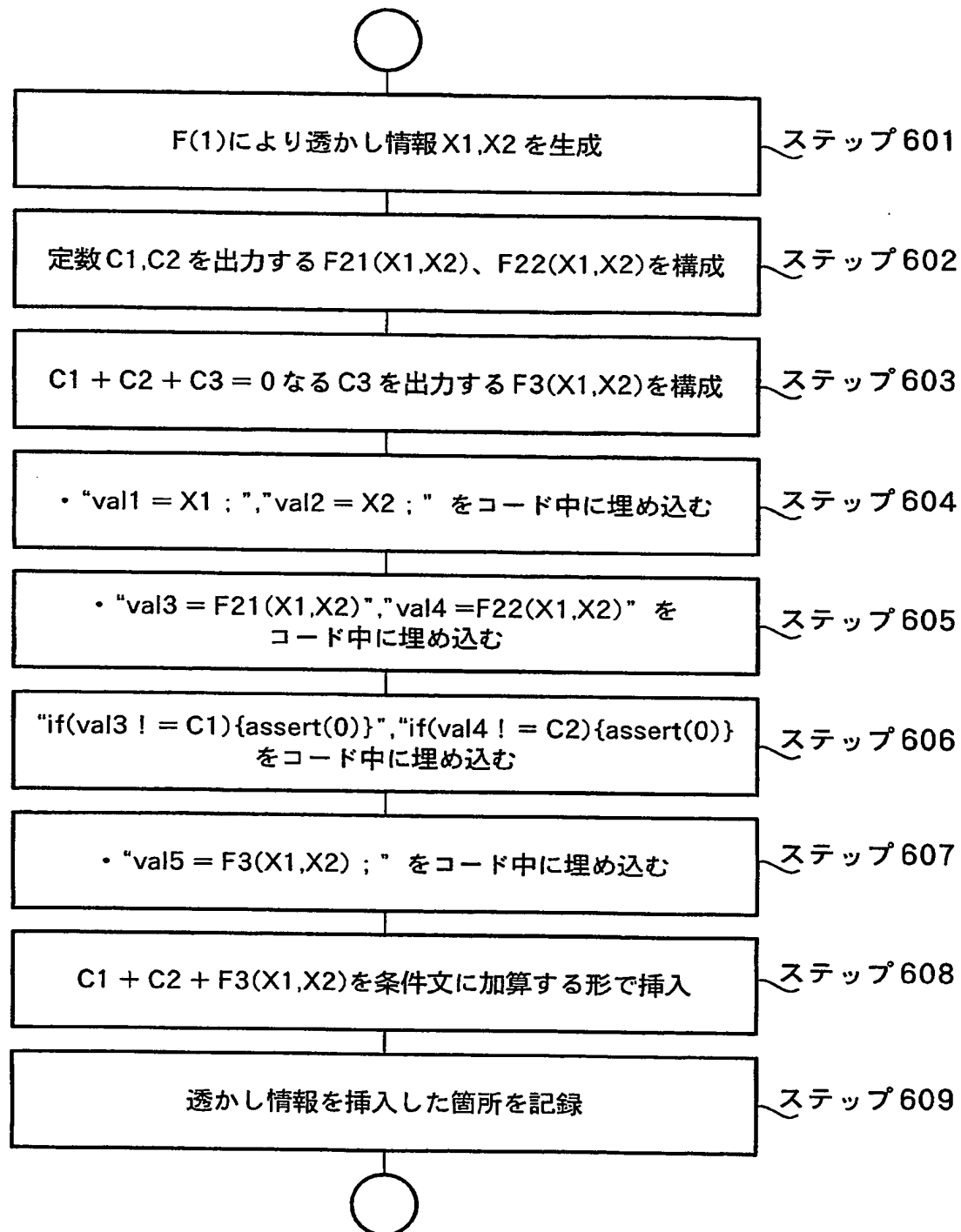


【図 6】





【図 7】



【図 8】

800a

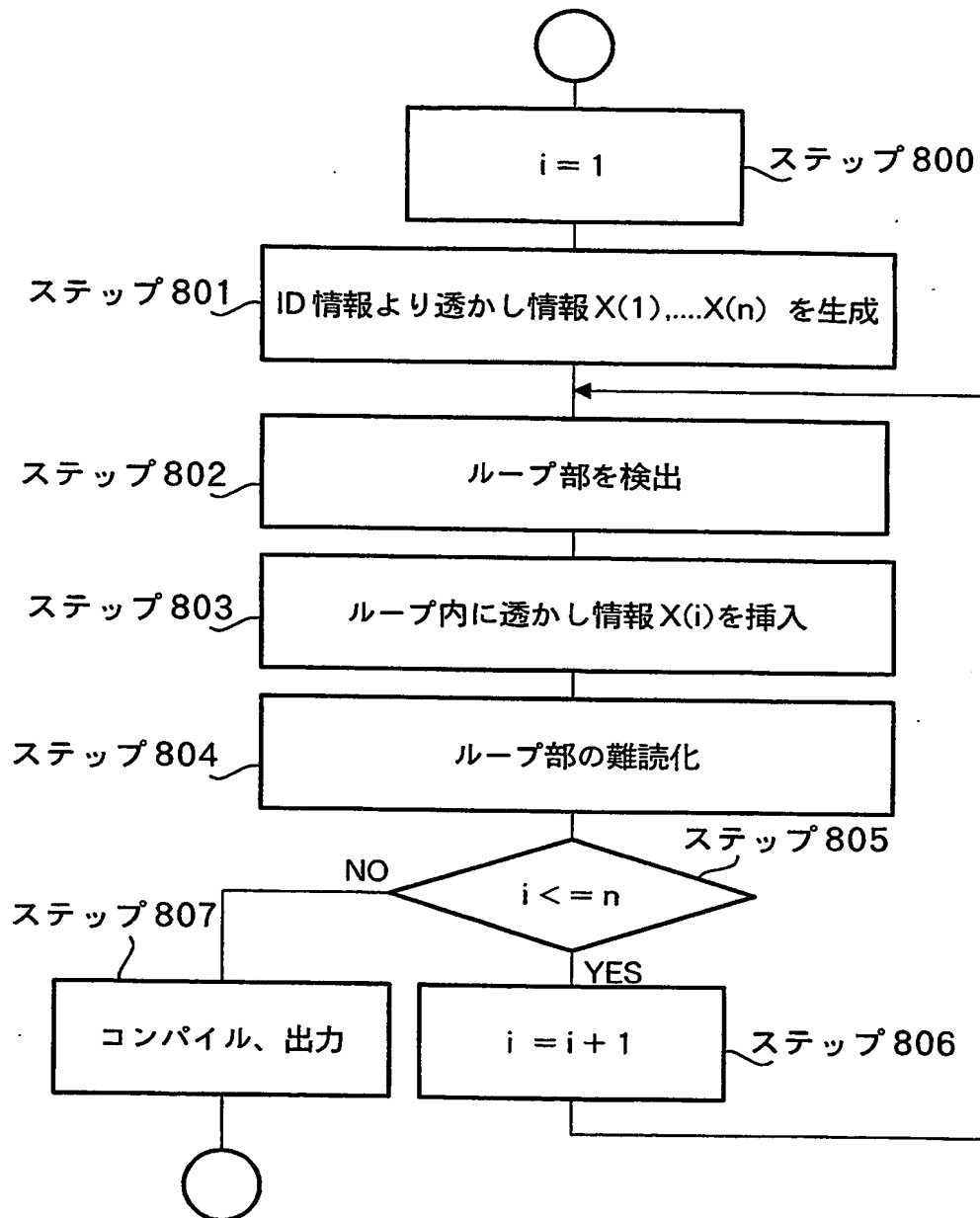
```
gcd(int x,int y){  
  int a=x,b=y,c;  
  while(b!=0){  
    a=a % b;  
    c=a; a=b; b=c;  
    if( a<0)a=-a;  
  }  
  return a;  
}
```

800b

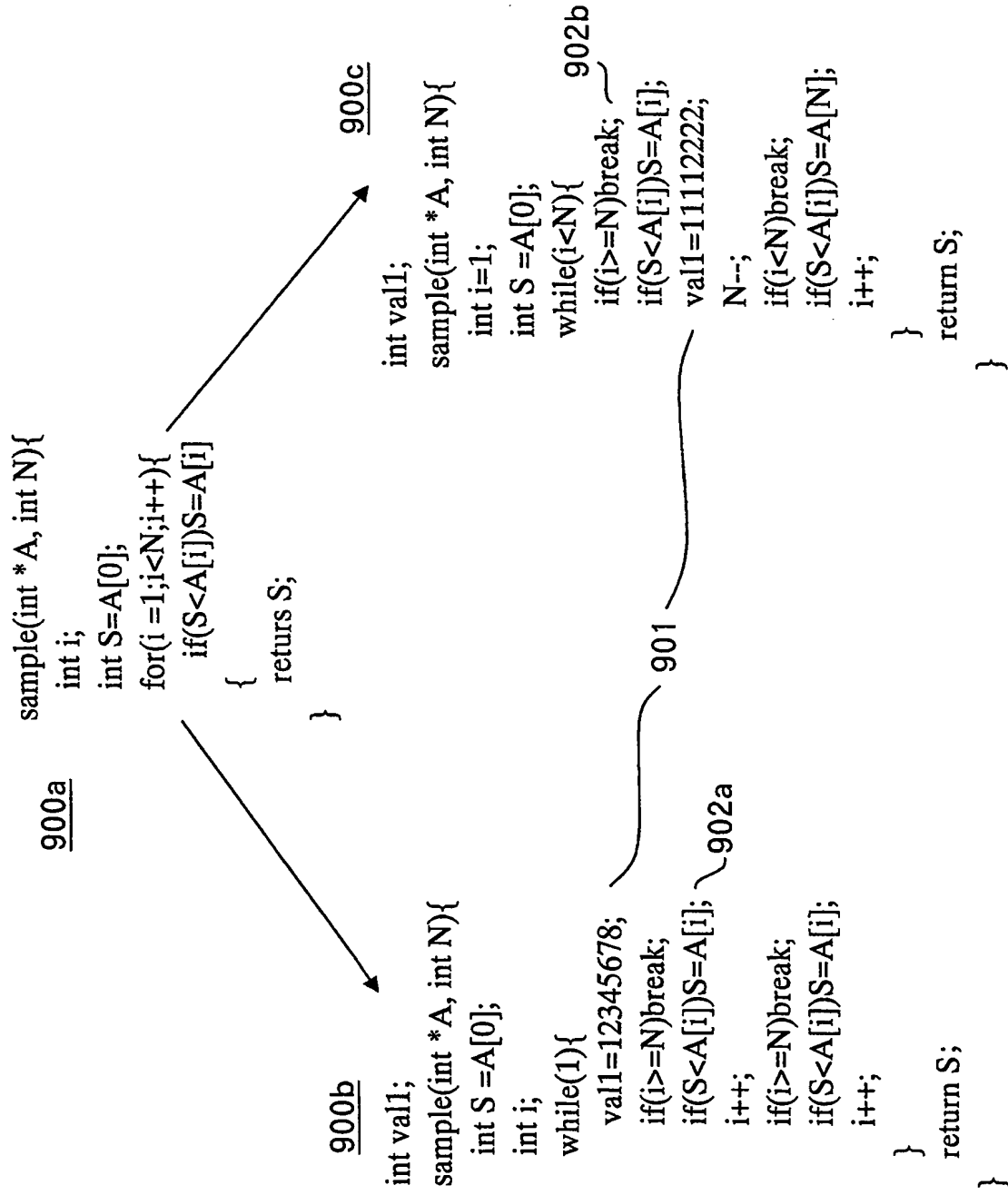
```
int val1=1234,val2=5678; ~701
```

```
gcd(int x,int y){  
  int a=x, b=y, c;  
  int val3=val1+0.195667*val2;  
  int val4=3.700972*val1+0.195667*val2;  
  int val5=5.601297*val1+0.195667*val2; } ~702  
  while(b!=0){  
    a=a % b;  
    c=a;a=b;b=c;  
    if(a<val3+val4+val5)a=-a; ~703  
    if(val3!=2345)a++;  
    if(val4!=5678)assert(0); } ~704  
  }  
  return a;  
}
```

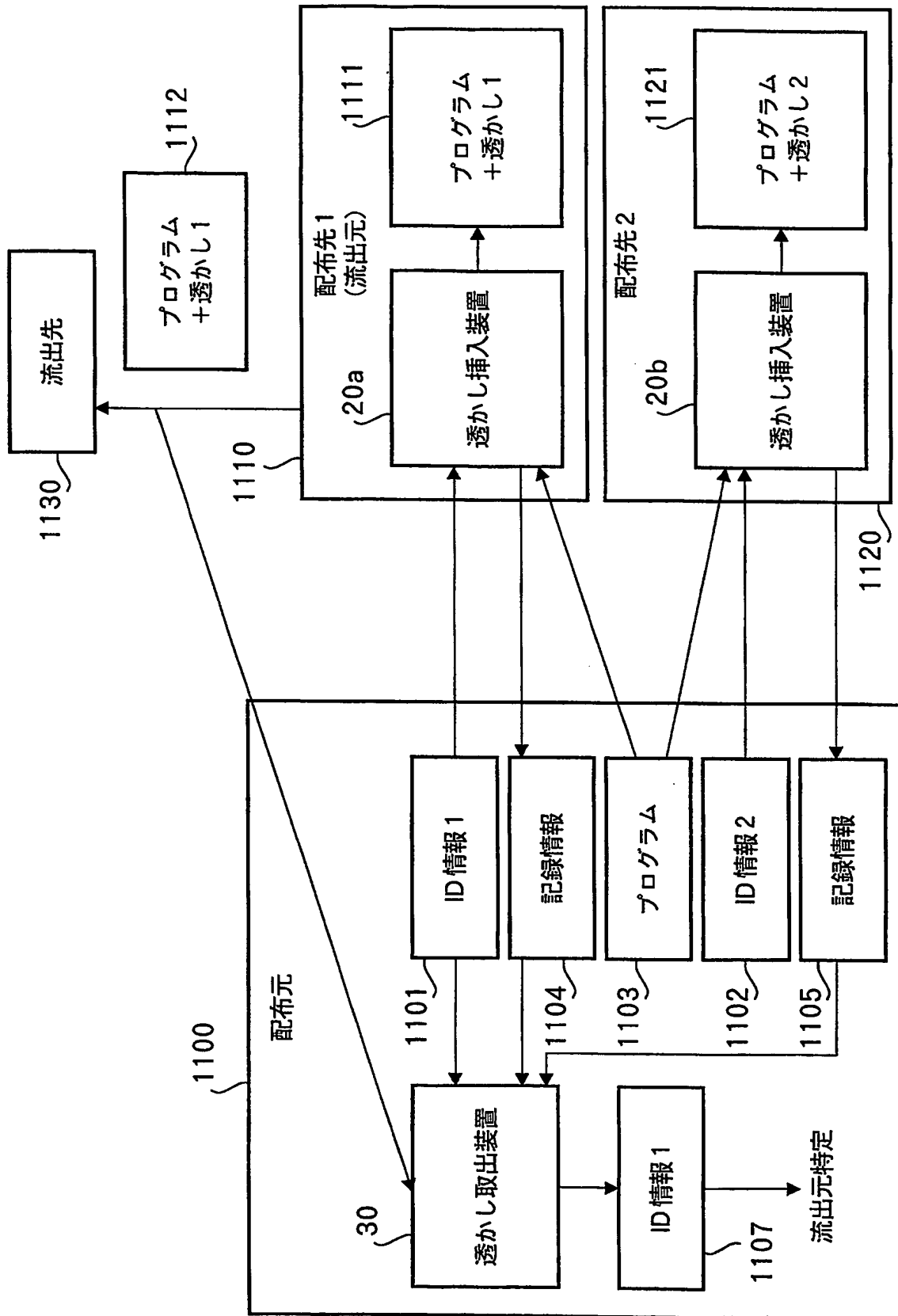
【図 9】



【図 10】



【図 11】



【書類名】 要約書

【要約】

【課題】 透かしの挿入箇所を特定されないように透かしを挿入することにより、透かし情報がなく、かつ正常に動作するプログラムを生成できないようにすること。

【解決手段】 本発明は、プログラムの配布先を一意に特定する I D 情報から透かし情報を生成し、前記透かし情報を前記プログラムに挿入し、前記透かし情報を用いたものであって、前記透かし情報が改ざんされた場合には、前記プログラムを正しく動作させないものであり、前記配布先毎に異なるコードを前記プログラムに挿入するようにすることにより、差分攻撃により透かしであるコードが検出されないようにした。

【選択図】 図 2

特願 2 0 0 2 - 3 1 1 8 1 5

出 願 人 履 歷 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[ 変更理由 ]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社